



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/901,286	07/09/2001	Hal Joseph Burch	2-9	7595
7590	02/10/2005		EXAMINER	ALOMARI, FIRAS B
Lucent Technologies Inc. Docket Administrator (Room 3J-219) 101 Crawfords Corner Road Holmdel, NJ 07733			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	09/901,286	BURCH ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Firas Alomari	2136

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

### **Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)  Responsive to communication(s) filed on 09 July 2001.

2a)  This action is **FINAL**.                            2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## **Disposition of Claims**

4)  Claim(s) 1-30 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5)  Claim(s) \_\_\_\_\_ is/are allowed.  
6)  Claim(s) 1-30 is/are rejected.  
7)  Claim(s) \_\_\_\_\_ is/are objected to.  
8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on \_\_\_\_\_ is/are: a)  accepted or b)  objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All    b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)  Notice of References Cited (PTO-892)  
2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3)  Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 01/31/2002.

4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_  
5)  Notice of Informal Patent Application (PTO-152)  
6)  Other: \_\_\_\_\_

## DETAILED ACTION

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-4, 6-19 and 21-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. US (2002/0032717) in view of Lee et al. US (2001/005360).

Regarding claims 1 and 16: Malan et al. discloses a method for tracing a sequence of packets to a potential source (Malan: Page 6; Paragraph 0117) thereof within a communications network the sequence of packets being received at a target host in said communications network at a received packet rate- the method comprising the steps of:

- Malan doesn't explicitly teach applying a burst load to each of one or more selected network elements in said communications network; For each selected network element measuring a change in said received packet rate in response to said application of said burst load to said selected network element. However Lee et al. teaches a method for measuring network congestion by sending relatively large packets (Lee: Page 2;

Paragraph 0041) and determining the packet loss amount or whether an error has occurred (Lee: Page 2; Paragraph 0035). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Malan with the teaching of Lee to include measuring network links congestion by sending a sending a relatively large packets and determining the packet loss amount or whether an error has occurred, since Lee states at paragraphs [0052-0056] that such modification would enable the system to provide the actual network state with monitoring method installed at only one system and with no special hardware, so that network load and expenses can be minimized and network utilization can be heightened.

- Determining said potential source of said sequence of packets based on said measured changes in said received packet rate. (Malan: Page 6; Paragraph 0119)

Regarding claims 2 and 17: Malan discloses the method of claim 1 wherein said communications network comprises the Internet. (Malan: FIG 1; the drawing shows the system connected to the Internet)

Regarding claims 3 and 18: Malan discloses the method of claim 1 wherein each of said selected network elements comprises a network link. (Malan: page 4, paragraph 0098)

Regarding claims 4 and 19: Malan doesn't explicitly teach the method of claim 3 wherein said step of applying a burst load to said network link comprises transmitting packets to a sub network of said communications network to initiate a responsive flow of packets through said network link. However Lee et al. teaches a method for measuring network congestion by sending relatively large packets (Lee: Page 2; Paragraph 0041) and determining the packet loss amount or whether an error has occurred (Lee: Page 2; Paragraph 0035). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Malan with the teaching of Lee to include measuring network links congestion by sending a sending a relatively large packets and determining the packet loss amount or whether an error has occurred, since Lee states at paragraphs [0052-0056] that such modification would enable the system to provide the actual network state with monitoring method installed at only one system and with no special hardware, so that network load and expenses can be minimized and network utilization can be heightened.

Regarding claims 6 and 21:Malan doesn't explicitly teach the method of claim 4 wherein said transmitted packets comprise UDP chargen requests. However Lee et al. teaches a method for measuring network congestion by sending UDP or TCP packets with an arbitrary character string (Lee: Page 2; Paragraphs 0041-0043). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Malan with the teaching of

Lee to allow Malan system to have enough packet length to be sent to the destination, since Lee states at paragraph [0036-0038] that such modification allow the system to apply the bandwidth formula and network links congestion to be calculated.

Regarding claims 7 and 22: Malan discloses the method of claim 1 wherein each of said selected network elements comprises a network router.(FIG 6 and FIG 8)

Regarding claims 8 and 23: Malan discloses the method of claim 1 further comprising the step of generating a map comprising routes from said target host to a plurality of subnetworks of said communications network. (Page 8; paragraph 0134)

Regarding claims 9 and 24: Malan discloses the method of claim 1 further comprising the step of eliminating said selected network element from consideration as said potential source of said sequence of packets when said change in said received packet rate meets a predetermined criterion.( Malan: Page 4; Paragraphs 0086-0091 and Page 6; Paragraph 0120)

Regarding claims 10 and 25: Malan discloses the method of claim 9 wherein said predetermined criterion comprises a determination of whether said change in said received packet rate is less than a predetermined threshold.( Malan: Page 4; Paragraphs 0086-0091 and Page 6; Paragraph 0119)

Regarding claims 11 and 26: Malan discloses the method of claim 9 wherein said step of eliminating said selected network element from consideration also eliminates from consideration one or more subnetworks of said communications network which are connected to said selected network element. (Page 6; Paragraph 0120)

Regarding claims 12 and 27: Malan discloses the method of claim 1 wherein said sequence of packets comprises a Denial-of-Service attack on said target host. (Page 6; Paragraph 0116)

Regarding claims 13 and 28: Malan discloses the method of claim 1 wherein said steps of applying said burst load. Measuring said changes in said received packet rate, and determining said potential source of said sequence of packets, are executed under the control of an automated algorithm. ( Page 8; Paragraph 0134)

Regarding claims 14 and 29: Malan discloses the method of claim 1 wherein said steps of applying said burst load and determining said potential source of said sequence of packets, are executed under the at least partial control of a human operator. (Page4 ; Paragraph0091 )

Regarding claims 15 and 30: Malan discloses the method of claim 14 further comprising the step of displaying information, said information including data representative of said measured changes in said received packet rate, to said human operator, for use by said human operator in exercising said at least partial control.(Page 4; Paragraph 0091 and page 6; Paragraph 0117 )

3. Claims 5 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al US (2002/0032717) and Lee et al. US (20001/0005360) as applied to claim 1 above, and further in view of Sharon et al. US (6,205,122).

Regarding claim 5 and 20: the combination of Malan and Lee doesn't teach the method of claim 4 wherein said transmitted packets are spoofed from an end of said network link closest to said target host. However Sharon teaches the spoofing of packets by changing the IP address of the packet to appear sent from a different machine on a different segment (Sharon: Col 12; lines 54-67).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system with the teaching of Sharon by spoofing the packets from a link closer to the target host, since Sharon states at Col 13; lines 1-7 that such a modification would allow the system to map an entire segment without the condition of physically residing on that segment.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571)272-7963. The examiner can normally be reached on Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari  
Examiner  
Art Unit 2136

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100